How Public-Private Collaborations Contribute to Cybercrime Disruption

By Derek Manky, Chief Security Strategist & Global VP Threat Intelligence | Board Advisor | Threat Alliances at FortiGuard Labs

Nearly 90% of organizations experienced at least one breach in the past 12 months. A myriad of ongoing challenges impact an organization’s susceptibility to cyberattacks, ranging from the constant and rapid adoption of new technologies to the ongoing cybersecurity talent shortage.

While there is no one-size-fits-all approach to enhancing organizational security measures and guarding against breaches, one thing is clear: A single entity cannot disrupt cybercrime alone, yet we must fight against our adversaries and hold them accountable for their actions. Establishing choke points on the chess board requires ongoing collaboration between the public and private sectors. Fortinet is proud to be part of numerous collaborative efforts to address cybercrime. The company is a founding member of the World Economic Forum Centre for Cybersecurity, a contributor to its Partnership Against Cybercrime (PAC), and a founding member of the Cybercrime Atlas.

The PAC launched in 2020 as a first step toward establishing a global architecture for promoting public-private cooperation to combat cybercrime. It offers a platform for sharing insights and exploring new approaches to drive successful collaboration against digital adversaries, bringing together businesses, national and international law enforcement agencies, and nonprofit organizations.

In 2023, the PAC created the Cybercrime Atlas, a first-of-its-kind initiative, leveraging the efforts of dozens of organizations to drive real impact by mapping threat actor activities and creating a chain of disruption in the cybercriminal ecosystem. Fortinet is a long-standing and active PAC community contributor and a founding member of the Cybercrime Atlas initiative.

From Operational to Actionable: Cybercrime Atlas Efforts Contribute to INTERPOL Arrests

The Cybercrime Atlas became operational earlier this year, two years after the initiative was introduced. Last month, the International Criminal Police Organization (INTERPOL) announced that it identified and arrested more than 1,000 suspects connected to major cybercrime operations with support from the Cybercrime Atlas initiative. This effort dismantled 134,089 malicious infrastructures and networks across 19 African countries, which had impacted more than 35,000 victims to date and resulted in $193 million in financial losses worldwide.

The Cybercrime Atlas initiative's investigations group, composed of more than 20 members, meets weekly to profile threat actors, review open-source intelligence regarding cybercriminal activities, correlate data, and identify potential disruption points. This information is then organized into intelligence packages to aid cybercrime takedown efforts.

In its first year of operation, Cybercrime Atlas contributors shared over 10,000 community-vetted and actionable data points and supported two cross-border cybercrime disruption efforts. The group created seven comprehensive intelligence packages on emerging threats that they shared with law enforcement to operationalize this actionable data. These intelligence packages from the Cybercrime Atlas initiative contributed directly to the success of this INTERPOL-led effort, which ultimately disrupted attacker operations and held adversaries accountable for their actions.

Strong Public-Private Collaborations Are Vital to Fighting Cybercrime

This recent takedown exemplifies how public-private collaborations like the Cybercrime Atlas initiative drive real impact in disrupting global cybercrime. Working across sectors and prioritizing threat intelligence sharing benefits the cybersecurity community, making us more resilient and effective collectively.

At Fortinet, we believe our corporate responsibility is to make the world safer and more sustainable, creating a digital world you can always trust. To deliver on this vision, we're committed to addressing cybersecurity risks for our customers and society.

No single individual or organization has complete insight into all the threats. Effectively disrupting cybercrime requires public and private organizations to work together, taking a coordinated and unified approach.

In addition to Fortinet’s involvement with the World Economic Forum PAC and Cybercrime Atlas initiative, we are committed to partnership and cooperation with global law enforcement agencies, government organizations, and industry organizations. Fortinet has been a trusted partner to INTERPOL and an active Global Cybercrime Expert Group member for nearly 10 years. The company also joined INTERPOL’s Gateway initiative in 2018, which offers a framework for sharing threat intelligence across organizations. This ongoing collaboration has resulted in adopting more substantial threat intelligence standards and protocols across the industry and impactful global cybercriminal takedowns. For example, in 2022, the FortiGuard Labs team provided evidentiary support to INTERPOL and African Member countries as part of the Africa Cyber Surge Operation to help detect, investigate, and disrupt cybercrime through coordinated law enforcement activities, using INTERPOL platforms, tools, and channels in close cooperation with AFRIPOL.

In addition to working with INTERPOL, Fortinet is actively involved with numerous public-private collaborations. The company is a long-standing member of the NATO Industry Cyber Partnership, a partner of NIST’s National Cybersecurity Excellence Partnership program, a founding member of the Cyber Threat Alliance, an official research partner with MITRE Engenuity’s Center for Threat-Informed Defense, and more.

As the global cybercrime landscape evolves, these collaborations will only become more critical to halting threat actors. The recent efforts of INTERPOL and the Cybercrime Atlas initiative are a strong example of how, when we work together, we can move faster and more effectively toward our collective goal of disrupting cybercrime.

Thank You.